WHAT IS CLAIMED IS:

1. Method of intercepting a voice/multimedia communication in a virtual private network, the method comprising:

setting up the voice/multimedia communication in the virtual private network, the communication composed of a plurality of data packets and signaling information;

extracting an identifying information for the voice/multimedia communication from the signaling information;

determining whether at least one participant in the voice/multimedia communication matches an intercept subject;

duplicating the plurality of data packets and the signaling information if it is determined that there is a match; and

re-originating the plurality of data packets and the signaling information in the virtual private network.

2. The method according to claim 1, further comprising encapsulating the data packets and storing the data packets in a database if there is a match.

3. The method according to claim 1, further comprising transporting the duplicated data packets to a law enforcement agency if there is a match.

4. The method according to claim 1, wherein the step of determining includes comparing an image/picture from the voice/multimedia communication with an image/picture of the intercept subject.

5. The method according to claim 4, wherein the step of determining is performed only until one or more predefined criteria are satisfied if there is no match between the image/picture from the voice/multimedia communication and the image/picture of the intercept subject.

6. The method according to claim 1, wherein the step of determining is performed for substantially all voice/multimedia communications occurring in the virtual private network if only an image/picture of the intercept subject is available.

7. The method according to claim 1, wherein the step of determining is performed only when the identifying information extracted from the signaling information matches an identifying information for the intercept subject.

8. The method according to claim 9, further comprising collecting and storing the identifying information of the intercept subject if the step of determining results in a match.

9. A virtual private network capable of intercepting a voice/multimedia communication composed of a plurality of data packets and signaling information being routed therethrough, the virtual private network comprising:

a call control entity configured to set up the voice/multimedia communication in the virtual private network and to extract an identifying information from the signaling information; and

a call intercepting server configured to determine whether at least one participant in the voice/multimedia communication matches an intercept subject and to duplicate the plurality of data packets and the signaling information if there is a match;

wherein the call control entity is further configured to re-originate the plurality of data packets and the signaling information in the virtual private network.

10. The virtual private network according to claim 9, wherein the voice/multimedia communication complies with one or more predefined signaling protocols, including a Voice Over IP (VoIP) protocol.

11. The virtual private network according to claim 9, wherein the signaling information complies with one or more predefined signaling protocols, including a Sessions Initiation Protocol (SIP) and a H.323 protocol.

12. The virtual private network according to claim 9, wherein format of the data packets complies with one or more predefined routing protocols, including a Real-time Transport Protocol (RTP).

13. The virtual private network according to claim 9, wherein the call intercepting server is a stand-alone server that is separate from the call control entity.

14. The virtual private network according to claim 9, wherein the call intercepting server is a functional feature within the call control entity.

15. The virtual private network according to claim 9, further comprising an access network including a plurality of access routers and a backbone network including a plurality of backbone routers, and the call control entity and the call intercepting server are connected to the access network and the backbone network.

16. The virtual private network according to claim 9, further comprising a virtual private network administrator configured to receive legal authorization for intercepting the/multimedia communication and to instruct the call control entity and the call intercepting server to carry out the interception.

17. The virtual private network according to claim 9, further comprising a database for storing the identifying information of the intercept subject if there is a match.

18. The virtual private network according to claim 9, wherein the call intercepting server determines if there is a match by comparing an image/picture from the voice/multimedia communication with an image/picture of the intercept subject.

19. The virtual private network according to claim 18, wherein the call intercepting server performs the determination only until one or more predefined criteria are satisfied if there is no match between the image/picture from the voice/multimedia communication and the image/picture of the intercept subject.

20. The virtual private network according to claim 9, wherein the call intercepting server performs the determination for substantially all voice/multimedia communications occurring in the virtual private network if only an image/picture of the intercept subject is available.

21. The virtual private network according to claim 9, wherein the call intercepting server performs the determination only when the identifying information extracted from the signaling information matches an identifying information for the intercept subject.